UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,479	03/07/2002	Eric Rescorla	730.39867X00	3321

22907 7590 01/31/2006

BANNER & WITCOFF
1001 G STREET N W
SUITE 1100
WASHINGTON, DC 20001

EXAMINER	
WON, MICHAEL YOUNG	
ART UNIT	**PAPER NUMBER**
2155	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/091,479	RESCORLA ET AL.	
	Examiner	Art Unit	
	Michael Y. Won	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed November 23, 2005.

2. Claims 1-27 has been cancelled and new claims 28-54 have been added.

3. Claims 28-54 have been examined and are pending with this action.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 28, 44, 46, and 49 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Although the examiner has noted with respect to Fig.3, that the "clustering state information" occurs after the receiving an acknowledgment message step, the examiner could not find conclusive evidence that the "clustering state information" occurs **responsive to** receiving an acknowledgment message as recited in claims 28, 44, and 46. Similarly, the examiner could not find

conclusive evidence that the "**in response to** the second acknowledgment, transmitting a third acknowledgment to the first node" as recited in claims 46. Finally, the examiner could not find conclusive evidence that the "transferring state information between SSL relays in the cluster **only in response** to an acknowledgment from the second node confirming receipt of transferred information" as recited in claims 49.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

5. Claim 33 recites the limitation "the third acknowledgment" in page 3 of the amendment. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 28-36, 39-40, and 42-54 are rejected under 35 U.S.C. 102(e) as being anticipated by Bruck et al. (US 6,691,165 B1).

INDEPENDENT:

As per ***claim 28***, Bruck teaches a method for clustered Secure Sockets Layer (SSL) acceleration comprising the steps of:

connecting at least two SSL (see col.27, liens 55-65) relays in a cluster (see Fig.2, #200 and see col.5, lines 33-35 & 38-40);

establishing a communication path between a first node and a second node via a first SSL relay of the cluster (see col.2, lines 63-65);

transferring information between the first node and the first relay SSL relay, the transferred information related to a communication from the first node to a second node (implicit: see Fig.3 and col.6, lines 22-33); and

clustering state information of the communication path (see col.6, lines 4-7; col.8, lines 45-48; and col.25, lines 27-32) in response to receiving an acknowledgment from the second node confirming receipt of the communication (see col.24, lines 58-66 and col.25, lines 9-14), the clustering comprising sharing the state information between the first SSL relay and at least a second SSL relay of the relay cluster (see col.10, lines 19-22 and col.24, lines 34-33), wherein the second SSL relay is capable of taking over the communication between the first and second node upon failure of the first SSL relay (see col.2, lines 49-54; col.3, lines 1-5; and col.6, lines 53-64).

As per ***claim 44***, Bruck teaches a system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node (see col.5, line 55: "client");

a second node (see col.5, lines 36-38: "back-end servers... application servers" & 55: "servers"); and

an SSL (see col.27, liens 55-65) relay cluster (see Fig.2, #200 and col.5, lines 33-35 & 38-40) for connecting the first node and second node (see col.2, lines 63-65) comprising:

a first SSL relay configured to cluster state information (see col.6, lines 4-7; col.8, lines 45-48; and col.25, lines 27-32) in response to a first acknowledgment from the second node confirming receipt of data transmitted from the first node (see col.24, lines 58-66 and col.25, lines 9-14); and

a second SSL relay configured to transmit a second acknowledgement to the first SSL relay upon receiving the state information (see col.10, lines 19-26: "911" message; col.15, lines 51-54; col.17, lines 18-29; and col.25, lines 1-8).

As per ***claim 46***, Bruck teaches computer readable medium storing computer readable instructions that, when executed by a processor, performs a method comprising:

establishing a connection between a first node and a second node via a first SSL (see col.27, liens 55-65) relay of an SSL relay cluster (see col.2, lines 63-65), wherein said SSL relay cluster comprises at least two interconnected SSL relays (see Fig.2, #200 and see col.5, lines 33-35 & 38-40);

receiving a data communication from the first node (implicit: see Fig.3 and col.6, lines 22-33);

transmitting the data communication to the second node (implicit: see Fig.3 and col.6, lines 22-33);

receiving a first acknowledgment from the second node confirming receipt of the data communication;

in response to the first acknowledgment (see col.24, lines 58-66 and col.25, lines 9-14), clustering state information of the established connection with at least a second SSL relay of the SSL relay cluster (see col.6, lines 4-7; col.8, lines 45-48; col.10, lines 19-22; col.24, lines 34-33; and col.25, lines 27-32);

receiving a second acknowledgment from at least the second SSL relay in the SSL relay cluster confirming successful clustering (see col.10, lines 19-26: "911" message; col.15, lines 51-54; col.17, lines 18-29; and col.25, lines 1-8); and

in response to the second acknowledgment, transmitting a third acknowledgment to the first node (see col.25, lines 1-8).

As per ***claim 49***, Bruck teaches an SSL relay, the SSL relay connected in a cluster of SSL relays, comprising:

a first interface (see Fig.3; col.6, line 65-col.7, line 7; and col.7, lines 16-21) for transferring information between a first node and the SSL relay(see col.27, liens 55-65);

a second interface (see Fig.3; col.6, line 65-col.7, line 7; and col.7, lines 16-21) for transferring information between a second node and the SSL relay (see col.27, liens 55-65);

a third interface (see Fig.3; col.6, line 65-col.7, line 7; and col.7, lines 16-21) for transferring state information between SSL relays (see col.27, liens 55-65) in the cluster

(see col.6, lines 4-7; col.8, lines 45-48; and col.25, lines 27-32) only in response to an acknowledgment from the second node confirming receipt of transferred information (see col.24, lines 58-66 and col.25, lines 9-14); and

a storage device, wherein the state information of an SSL connection between the first node and the SSL relay is shared across each SSL relay in the cluster (see col.10, lines 19-22 and col.24, lines 34-33), any of the SSL relays in the cluster capable of taking over all connections of another SSL relay in the cluster, therefore providing no interruption in the transfer of information should any of the SSL relays in the cluster fail (see col.2, lines 49-54; col.3, lines 1-5; and col.6, lines 53-64).

DEPENDENT:

As per ***claims 29, 45, 48, and 50***, which depend on claims 28, 44, 46, 49, respectively, Bruck further teaches wherein the first node comprises a client and the second node comprises a server (see col.2, lines 63-65).

As per ***claim 30***, Bruck teaches of further comprising transferring information associated with communications between the first node and a second to the second SSL relay transparently upon failure of the first SSL relay (see col.2, lines 49-54 & 63-65 and col.8, lines 62-65).

As per ***claim 31***, Bruck teaches of further comprising transmitting the communication from the first node to a second SSL relay and from the second SSL relay to the second node transparently upon failure of the first SSL relay (see claim 28 and 30 rejections above).

As per ***claim 32***, Bruck further teaches wherein the data communication comprises data being transferred between the first node and the second node (see col.2, lines 63-65).

As per ***claim 33***, Bruck further teaches wherein **the** third acknowledgment confirms receipt of data communication by the second node (see col.24, lines 58-66)

As per ***claim 34***, Bruck teaches of further comprising sharing an SSL session cache across all of the at least two SSL relays (see col.16, line 66-col.17, line 6).

As per ***claim 35***, Bruck teaches of further comprising clustering an SSL session resumption between the first node and the one of the at least two SSL relays (see col.28, lines 41-55)

As per ***claim 36***, Bruck teaches of further comprising clustering cryptographic keying information across all of the at least two SSL relays (see col.13, lines 40-44).

As per ***claim 39***, Bruck does not teach of further comprising clustering a current key schedule (see col.13, lines 40-44).

As per ***claim 40***, Bruck teaches of further comprising clustering a key and an offset into a key stream (see col.13, lines 40-44).

As per ***claim 42***, Bruck teaches of further comprising clustering data from a partial record corresponding to data from either the first or second node (see col.24, lines 51-66).

As per ***claim 43***, Bruck teaches of further comprising clustering a record size before the record is transmitted (see col.24, lines 53-55).

As per ***claim 47***, Bruck does not teach wherein the (SSL) relay assumes the first SSL relay's responsibilities upon failure of the first SSL relay (see col.2, lines 49-54 & 63-65 and col.8, lines 62-65).

As per ***claims 51-54***, Bruck further teaches wherein the first interface and the second interface and the third interface are the same (implicit: see col.5, line 51-col.6, line 4).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 37, 38, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruck et al. (US 6,691,165 B1) in view of Weinstein et al. (US 6,094,485 A).

As per ***claim 37***, although Bruck teaches of further comprising clustering a key (see claim 36 rejection above), Bruck does not explicitly teach of clustering a current Cipher Block Chaining (CBC) residue. Weinstein teaches of clustering a current Cipher Block Chaining (CBC) residue (see col.8, lines 5-10 and col.9, lines 24-28).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing Cipher Block Chaining (CBC) residue within the method for clustered Secure Sockets Layer (SSL) acceleration because such implementation would provide a strong encryption scheme applicable with SSL.

As per ***claim 38***, Bruck does not teach of further comprising clustering a sequence number. Weinstein teaches of further comprising clustering a sequence number (see col.9, lines 29-34).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing clustering a sequence number within the method for clustered Secure Sockets Layer (SSL) acceleration because such implementation would provide a strong encryption scheme applicable with SSL.

Weinstein teaches of further comprising clustering a current key schedule (see col.17, line 2 to col.18, line 59).

As per ***claim 41***, Bruck does not teach of further comprising clustering a cipher state. Weinstein teaches of further comprising clustering a cipher state (see col.11, lines 17-19).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing clustering a cipher state within the method for clustered Secure Sockets Layer (SSL) acceleration because such implementation would continue to provide

transparent communication between the nodes even in the event of failure to one SSL relay.

Response to Arguments

8. Applicant's arguments with respect to claims 27-54 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Y. Won whose telephone number is 571-272-3993. The examiner can normally be reached on M-Th: 7AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael Won

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER

January 24, 2006